Before the

Committee on the Judiciary

Subcommittee on Crime, Terrorism,
Homeland Security, and Investigations

United States House of Representatives

The Electronic Communications Privacy Act (ECPA), Part 2:

Geolocation Privacy and Surveillance

April 25, 2013

Statement of

Mark Eckenwiler
Senior Counsel
Perkins Coie LLP

I. INTRODUCTION

Chairman Sensenbrenner, Ranking Member Scott, and distinguished members of the Subcommittee, thank you for convening this hearing. It is an honor to appear before you today to discuss the important legal and technical issues raised by law enforcement access to wireless user location data.

Let me say at the outset that these comments reflect my personal views. I am not speaking for or on behalf of any client or group of clients, nor for my former colleagues at the Department of Justice. Instead, I offer my personal observations, drawn from over 16 years of working with the Electronic Communications Privacy Act (ECPA) while with the Justice Department and, more recently, in the course of representing service providers in private practice.

II. TYPES OF LOCATION DATA AVAILABLE FROM WIRELESS CARRIERS

To understand the issues surrounding law enforcement access to carrier-held location data, it is essential to start with the technology, not the law. Law enforcement typically seeks two distinct types of location data from wireless carriers: cell-site location information and precision location data.

A. Cell-Site Location Information (CSLI). As you know, cellular providers rely upon a network of antennas to provide service across large coverage areas. Whenever a user places or receives a voice call (or sends or receives a text message), the radio portion of that communication is transmitted between the customer's handset and a nearby tower. If the user moves in the course of a voice call—such as when traveling on the highway—the call may be seamlessly "handed off" to one or more other towers in sequence as the handset moves through different coverage areas.

Spacing between towers is determined primarily by the amount of network activity (and thus by the number of users) in a given area. In sparsely populated regions, cell towers are widely spaced, with each typically serving a coverage area several miles in radius. In suburban areas with moderate population density, carriers place towers closer together, with each having a service radius of a mile or less. Antennas in center cities are clustered even more tightly, with cell towers in the most densely populated areas (such as midtown Manhattan) spaced every 200 meters or less.

In suburban and urban areas, the coverage area for a given cell tower is typically subdivided into multiple sectors (or tower "faces"). In these cases, there are typically three 120-degree sectors, each with its own antenna. (To visualize this configuration, imagine a clock face divided into thirds from 10 to 2, 2 to 6, and 6 to 10. Each "pie slice" represents the coverage area for a given antenna.) Towers in sparsely populated areas, by contrast, normally have a single omnidirectional antenna.

Whenever a user places or receives a voice call (or sends or receives a text message), the network handling that communication—which may be the customer's home network, or another network with which the customer's carrier has a roaming agreement—creates a record of the first cell tower that handles the call or text message. If the tower coverage area is divided into multiple sectors, the stored cell-site location information (CSLI) record also indicates which

particular antenna handled the communication. Most, but not all, carriers also record the last tower (and, where applicable, sector) handling a voice call. Because text messages are short, and thus are transmitted almost instantaneously, they pass through only a single antenna.

The degree to which CSLI reveals the location of a user's phone varies for several reasons. First, these records do not provide grid coordinates for the phone itself; rather, they indicate which nearby antenna transmitted a communication associated with that handset. Because tower spacing varies enormously, the radius of corresponding tower coverage does as well, and therefore the projected area from where a call was placed will likewise vary.

In heavily populated urban areas, CSLI can—subject to the further limitations discussed below—place a handset in an area of approximately 1,000 square meters. In suburban areas with towers spaced further apart, CSLI may suggest an area of a square mile or more. Tower data from rural areas, by contrast, provides only very broad location data often covering dozens of square miles or more.

Other factors also contribute to the general imprecision of CSLI. For example, the boundaries between the sectors of an individual cell tower, as well as the boundaries between areas served by different towers, are neither precise nor fixed. Records showing communications activity alternating between two adjacent coverage areas may indicate handset movement back and forth between the areas, or may instead result from the activity of a non-moving user in an area of overlapping coverage.

More importantly, a particular communication is not always handled by the closest tower. Both natural terrain features (*e.g.*, hills and valleys) and man-made structures interfere with line-of-sight radio transmission. Weather conditions, including precipitation or even humidity level, also may affect signal propagation.

At times, the carrier antenna closest to the user's handset may even be entirely unavailable. This can result from local, temporary equipment or network outages, or simply from network congestion. For example, when highway traffic backs up at a toll plaza or accident scene, the nearest tower's capacity may be saturated by unusually high activity levels. In these circumstances, the next user trying to make a call may only be able connect to a more distant, less burdened tower; the resulting CSLI record will indicate usage of the latter, creating the misleading impression that the handset was closer to that tower than to any other.

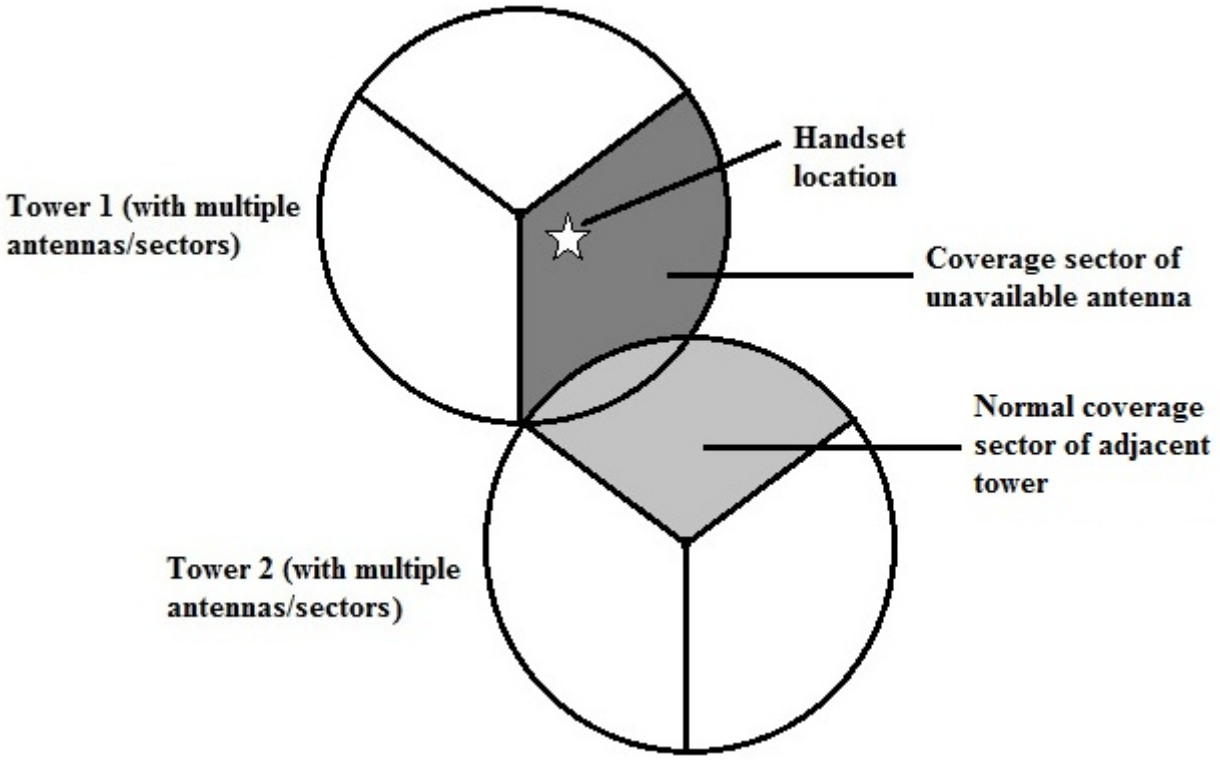

Figure 1

In Figure 1 above, the star represents a hypothetical handset location; the dark area represents the normal, but temporarily unavailable, coverage area for the closest antenna on Tower 1; and the light gray area depicts the normal coverage area for an adjacent tower's sector. Activity handled by Tower 2 would create a record associating the handset with the light gray area, even though the phone was outside that sector and closer to Tower 1.

Some commentators assert that the increasing use of "microcells" with smaller coverage areas renders CSLI functionally equivalent to GPS or other more precise location technologies. These claims are misleading. User-owned microcells – such as those purchased and installed by home customers – do not expand the network of towers available to the general population. Rather, these microcells are usable only by their owners, and therefore cannot provide service to, let alone identify the location of, the millions of other cell phone users.

B. Laws Restricting Disclosure of CSLI to Government Agencies: The Electronic Communications Privacy Act (ECPA) is the main federal statute regulating communications privacy. ECPA draws numerous distinctions between

- real-time (prospective) collection and access to historical records;
- communications content and non-content records; and
- transactional non-content records and more limited subscriber records.

Depending on the type of information sought and the manner in which it is to be collected, ECPA requires varying forms of compulsory process. These range from subpoenas—issued by a

prosecutor (or, in some cases, an investigative agency) on the comparatively low standard of relevance—up through various types of increasingly demanding court orders—with wiretap orders (based on probable cause and other special requirements) at the other end of the spectrum.

1. Access to Stored CSLI

As originally enacted in 1986, ECPA allowed the government to obtain any stored non-content record about a communications provider's customer using a grand jury, trial, or administrative subpoena. As part of the 1994 Communications Assistance for Law Enforcement Act (CALEA), however, Congress amended ECPA to divide non-content records into two categories.

The first of these categories, often referred to informally as "basic subscriber information," remains available in response to a subpoena.[1] These records—explicitly enumerated in an exhaustive list of six categories—include the customer's name, address, account identifier, length of service, and method of payment. Except for "local and long distance telephone connection records, or records of session times and durations," however, this category does not include records about specific user activity.

Instead, when law enforcement seeks to compel a service provider to disclose other stored non-content records, it must apply for a unique type of court order that was created in the 1994 amendment to ECPA.[2] To obtain this so-called "2703(d) order" (named for the section of the statute where it resides), the government must

> offer[] specific and articulable facts showing that there are reasonable grounds to believe that … the records or other information sought, are relevant and material to an ongoing criminal investigation.

As explained in the report from this Committee, "[t]he intent of raising the standard for access to transactional data is to guard against 'fishing expeditions' by law enforcement."[3] Advocating strongly in favor of this raised standard during an August 11, 1994 joint House-Senate committee hearing on the legislation,[4] the Executive Director of the Electronic Frontier Foundation described the proposal as follows:

> Chief among these new protections is an enhanced protection for transactional records from indiscriminate law enforcement access.

---

[1] *See* 18 U.S.C. § 2703(c)(2).

[2] *See* § 2703(d).

[3] H. Rep. No. 827, 103d Cong., 2d Sess., at 31 (Oct. 4, 1994).

[4] *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services, 1994: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 103d Cong., 2d Sess. 160-61 (1994) (prepared statement of Jerry J. Berman, Executive Director, Electronic Frontier Foundation).

> ... Provisions in the bill recognize that this transactional information created by new digital communications systems is extremely sensitive and deserves a high degree of protection from casual law enforcement access which is currently possible without any independent judicial supervision. ...
>
> In order to gain access to transactional records ... law enforcement will have to prove to a court, by the showing of "specific and articulable facts" that the records requested are relevant to an ongoing criminal investigation. This means that the government may not request volumes of transactional records merely to see what it can find through traffic analysis. Rather, law enforcement will have to prove to a court that it has reason to believe that it will find specific information relevant to an ongoing criminal investigation in the records it requested. ...
>
> Court order protection will make it much more difficult for law enforcement to go on "fishing expeditions" through online transactional records, hoping to find evidence of a crime by accident. ...
>
> The most important change that these new provisions offer is that law enforcement will: (a) have to convince a judge that there is reason to look at a particular set of records, and; (b) have to expend the time and energy necessary to have a United States Attorney or District Attorney actually present a case before a court.

An overwhelming majority of courts, including the federal Third Circuit Court of Appeals, has found that historical "CSLI from cell phone calls is obtainable under a § 2703(d) order."[5] Although a handful of lower courts have held that section 2703(d) does not apply to stored CSLI, this view has failed to win broader acceptance.[6] Many of these same lower court judges have also argued that historical CSLI is protected by the Fourth Amendment, and that a warrant is therefore necessary to compel such third-party records. Here, too, this represents a minority position; so far as I am aware, no federal court has ever granted a motion to suppress CSLI on these or any other grounds, despite attempts by numerous criminal defendants.[7]

---

[5] *In re Application*, 620 F.3d 304, 313 (3d Cir. 2010).

[6] Courts adopting this minority view point to the exclusion of "any communication from a tracking device (as defined in section 3117 of this title)" from ECPA's definition, at 18 U.S.C. § 2510(12)(C), of "electronic communication." (As noted by the Third Circuit, this view fails to distinguish between a communication itself – such as a phone call – and data *about* the communication, such as CSLI.) The minority view has the perverse consequence of excluding CSLI entirely from ECPA's protections, meaning that the government could compel CSLI using lesser compulsory process such as a subpoena.

[7] *See, e.g., United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012) (finding no Fourth Amendment interest); *see also United States v. Jones*, 2012 WL 6443136 at *5 & n.9 (D.D.C. Dec. 14, 2012) (collecting cases).

2. Prospective Collection of CSLI

CSLI acquired in real time is qualitatively the same (and thus its value is subject to the same practical limitations) as historical CSLI. The rules governing real-time government acquisition of CSLI from wireless carriers are, however, much less clear.

The pen register statute permits the government to obtain a court order authorizing ongoing collection of non-content "dialing, routing, addressing, or signaling information,"[8] information that would normally include CSLI. However, CALEA states that

> with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127), such call-identifying information [delivered by a carrier to the government] shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number) ….[9]

This restriction creates a gap in the statutory framework: although it declares which type of process may not be used (*i.e.*, a bare pen register order), it does not prescribe the types of court orders that may be used. (Moreover, the other major federal statute governing real-time surveillance—the far more demanding Wiretap Act—does not apply because it regulates only the collection of communications contents.[10])

In an effort to fill this gap, prosecutors began to apply for court orders under the combined authority of the pen register statute and section 2703(d) (which, as discussed above, requires a higher showing) on the grounds that such orders are not "solely pursuant" to pen register authority. Beginning in 2005, however, lower court judges started to reject these so-called "hybrid" orders. While some of these courts based their objections on obvious misunderstandings of the technology and kinds of data involved,[11] others reasoned that section 2703(d)—located in the Stored Communications Act,[12] and lacking provisions that address duration and other aspects of real-time surveillance—could not be used to collect information prospectively. These courts concluded that the government needs to use a search warrant, not

[8] 18 U.S.C. § 3127(3).

[9] 47 U.S.C. § 1002(a)(2).

[10] *See* 18 U.S.C. §§ 2510(4) (defining "intercept" to mean "the aural or other acquisition of the contents" of a protected communication) & 2510(8) (defining "contents" to mean "any information concerning the substance, purport, or meaning of [a] communication").

[11] The most obvious example of this phenomenon is *In re Application*, 402 F. Supp. 2d 597 (D. Md. 2005), in which the court confuses CSLI with GPS data. *See id.* at 599.

[12] Chapter 121 of Title 18 is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

because the Fourth Amendment requires it, but rather because a search warrant is the only available mechanism.[13]

Courts remain sharply divided on this question, with practices varying from district to district (and, in some cases, from one judge to another within a single federal district). Even courts endorsing the hybrid theory have called upon Congress to resolve the issue.[14]

C. Precision Location Information (PLI). Beginning in 1997, the FCC adopted regulations requiring cellular carriers to be able to locate wireless 911 callers. Phase I of this rulemaking—known as Enhanced 911 or simply E-911—required carriers to be able to deliver a 911 caller's cell-site and sector information (*i.e.*, CSLI) to the "public safety answering point" (*i.e.*, the 911 call center). Because of the inherent limits on the precision of CSLI, E-911 Phase II (in effect today) requires carriers to be able to deliver more precise location information.

In imposing these obligations, the FCC permitted carriers to choose either of two different methodologies for complying:

1. **Handset-based location technology** relying on special hardware or software in the mobile phone itself. U.S. carriers opting for such a "handset solution" have chosen to use Global Positioning System (GPS) technology, in which the phone calculates its position based on signals received from overhead GPS satellites.

2. **Network-based location technology** in which the work of calculating a phone's position occurs not on the handset, but rather in the carrier's network. This "network solution" typically involves measuring the time required for a test signal to travel between the handset and detection devices on cell towers in the vicinity. Using the known locations of those towers and the different timing information, software in the carrier's network is able to calculate a position for the phone. (This process, technically known as "multilateration," is often referred to informally as "triangulation.")

Generally speaking, the regulations require such E-911 Phase II location information to be accurate to within 50-300 meters.[15]

Contrary to popular belief, carriers do not collect these types of precise location information (PLI) on consumer-level users in the ordinary course of business.[16] As a result, historical PLI from these technologies is not available to law enforcement.

---

[13] Typical of this line of cases is *In re Application*, 497 F. Supp. 2d 301 (D.P.R. 2007).

[14] *See In re Application*, 632 F. Supp. 2d 202, 211 (E.D.N.Y. 2008) ("District courts across the country are divided on an issue that requires balancing the Government's investigatory needs with citizens' right to privacy. Absent clarity from Congress, this division and inconsistency in outcomes will continue because the issue is one about which reasonable judges can, and obviously do, disagree."); *In re Application*, 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006).

[15] The applicable regulation (47 C.F.R. § 20.18(h)) lays out a complex set of criteria, including several deadlines for compliance across increased geographic areas. In general, handset-solution phone location data must be more precise than network-solution data.

However, law enforcement may nevertheless seek PLI on a prospective basis. Because ECPA itself provides no clear mechanism for compelling this type of information, it is common for prosecutors to obtain a search warrant under Federal Rule 41 or a state equivalent. In doing so, some prosecutors rely on the explicit "tracking device" provisions of Rule 41, while others rely upon the Rule's well-established history of use as a general means of conducting ongoing evidence collection.[17] These may appear either in the form of stand-alone warrants, or as supplemental authority incorporated into a wiretap order.[18]

III. ISSUES DESERVING CONGRESSIONAL ATTENTION

As suggested above, there are several areas in which the current legal framework is not entirely satisfactory. These include the following:

1. Hybrid orders. Easily the source of greatest controversy, the government's use of hybrid orders—*i.e.*, court orders combining the authority of the pen register statute and the "specific and articulable facts" test of section 2703(d) —has led to a sharp divide among lower federal courts. Greater clarity in this area would be an enormous benefit to the service provider community; providers have a substantial interest in knowing with certainty the boundaries of what is lawful, in protecting their customers' privacy, and in avoiding potential civil liability.

2. "Tower dumps". Instead of seeking historical CSLI for the identified phone of a specific target, prosecutors sometimes use a section 2703(d) order to seek all records associated with calls handled by a given tower for a specified interval of time (usually corresponding to the date and time of an unsolved crime). These so-called "tower dumps" can be essential to identifying suspects in certain kinds of crimes such as bank robberies,[19] but almost invariably involve disclosure of large numbers of user records. The volume of information varies enormously according to time of day, the size of the

---

[16] Many carriers do, however, offer so-called "fleet management" services to business customers at additional cost. In some cases, these services—intended for locating a company's delivery drivers, construction site supervisors, and the like—permit not only real-time monitoring but also review of historical PLI.

[17] Prior to the 2006 addition of tracking device provisions, prosecutors used Rule 41 to obtain warrants when needed to authorize the use of such devices. This practice flowed directly from the Supreme Court's directive in *United States v. Karo*, 468 U.S. 705, 718 (1984), to seek a warrant for certain tracking device uses. Prior to the 1986 enactment of the pen register statute, the Supreme Court likewise read Rule 41 as "sufficiently flexible" for use in authorizing prospective surveillance of dialed telephone numbers. *United States v. New York Telephone Co.*, 434 U.S. 159, 169 (1977). And the federal circuits are unanimous in relying on Rule 41 as authority for issuance of surreptitious video surveillance warrants, even though the Rule contains no explicit provisions contemplating this use. *See, e.g., United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (*en banc*); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 252 (5th Cir. 1987).

[18] *See, e.g., United States v. Ortega-Estrada*, 2008 WL 4716949 at *14 (N.D. Ga. Oct. 22, 2008).

[19] *See, e.g.*, Criminal Complaint, *United States v. Capito* (D. Ariz. Mar. 12, 2010) (describing, at pp. 12-15, the use of tower dump data to identify the phones used by suspects at four separate armed bank robberies), available at http://tinyurl.com/towerdump.

requested time frame, and the type of area (rural, suburban, or urban) at issue, but can reveal thousands or even tens of thousands of records.[20]

Given the potential for disclosure of such customer information, the Committee may wish to consider the desirability of additional statutory protections such as limits on the number of records or the length of the time window requested, or protocols for sealing or destroying voluminous non-pertinent records.

3. Warrants or orders to surveil unidentified phones contacting a target phone. Prosecutors at the state level sometimes apply for warrants or court orders that authorize monitoring the location not only of a named target phone (as to which they must establish probable cause), but also of any other phone that contacts (or is contacted by) the target phone during the authorized period of surveillance. This is a troubling practice: it allows for location monitoring of an undetermined number of phones not identified in the warrant, and on the questionable assumption that even a single contact with the target phone constitutes evidence of criminal activity.

   In light of the potential for significant, unjustified privacy invasions—for example, from misdialed numbers or calls from family members or others uninvolved in criminal activity—the Committee should carefully consider whether additional safeguards are required to limit or prohibit these types of orders.

4. Legal framework for real-time PLI monitoring. More generally, the Committee may wish to examine the adequacy of the current, somewhat ad hoc use of Rule 41 to authorize real-time law enforcement access to PLI. Specific areas for potential review include the following:

   a. *Whether the "tracking device" provisions are adequate for use in this area*. Rule 41 requires that a "tracking device" warrant be issued in the district where the device is "install[ed]."[21] Although this poses no problems in the case of the physical tracking devices clearly contemplated by the Rule's drafters, it is a potentially serious obstacle in situations where (1) the court believes the tracking device provisions strictly apply to cell phone location and (2) the applicant cannot attest that the phone is within the district at the time of application. Indeed, since the objective of such applications is to learn the location of the target phone through court-authorized electronic surveillance, this requirement generally creates a Catch-22.

   b. *Burden on service providers, and compensation therefor*. Rule 41 does not impose any explicit limit on how often law enforcement may request PLI in the course of executing a prospective warrant. In many instances, manual intervention by carrier personnel is necessary, often on nights and weekends, making frequent

[20] According to the *Capito* complaint, "[i]nvestigators used the four most rural [bank robbery] locations in order to minimize the amount of extraneous telephone data that would likely be obtained …." *Id.* at 13.

[21] Fed. R. Crim. P. 41(b)(4).

requests extremely burdensome. Moreover, Rule 41 contains no provisions for compensating carriers for their often substantial compliance costs.

c. *Emergency requests*. Both the Wiretap Act and the pen register statute include express language allowing law enforcement to conduct surveillance in emergencies without first obtaining court authorization.[22] Each of these statutes requires the government to apply to a court for retroactive authorization within 48 hours. By contrast, Rule 41 contains no such emergency compulsion provision.

IV. CONCLUSION

ECPA and its companion statutes currently provide significant privacy protection for wireless customers' location data. However, at least one gap in the statute has provoked widespread disagreement among federal judges, and other practical and procedural difficulties have emerged over time. Because these problem areas have a direct impact on user privacy, on service providers' compliance practices, and on our Nation's law enforcement efforts, the Committee deserves great credit for recognizing the need to re-examine the existing legal authorities and consider potential solutions.

Thank you for this opportunity to testify. I look forward to your questions.

[22] *See* 18 U.S.C. §§ 2518(7) (wiretap emergency authority) & 3125 (pen register).